Cisco BTS 10200 Softswitch Release Notes for Release 3.5 V02

The Cisco BTS 10200 Softswitch is a class-independent software switch (softswitch) that provides next-generation integrated voice and data switching solutions for packet networks.

These release notes for the Cisco BTS 10200 Softswitch describe the enhancements and new features provided in Release 3.5 Version 02 (Release 900-03.05.02.Q00). This release is targeted for North American T1 and cable customers. If you are not a North American customer, contact your Cisco representative for more information.

Please see the "Limitations and Restrictions" section on page 4 for important information about the approved use of this software release.

These release notes are updated as needed. Please read the applicable sections in their entirety, because they contain important operational information that can impact your network.

Contents

This document includes the following sections:

- System Requirements, page 2
- New and Changed Information, page 4
- Caveats, page 8
- Documentation Updates, page 14
- Related Documentation, page 14
- Obtaining Documentation, page 15
- Obtaining Technical Assistance, page 16

CISCO SYSTEMS

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2002. Cisco Systems, Inc. All rights reserved.

CISCO CONFIDENTIAL

System Requirements

The Cisco BTS 10200 Softswitch consists of the following equipment:

- Call Agent/Feature Server (CA/FS)—Two application servers, each with four CPUs.
- Element Management System/bulk Data Management System (EMS/BDMS) server—Two administration processors, each with one CPU.
- Two switch routers.
- Power distribution unit (PDU) for DC systems.

  DC-powered systems require two (redundant) feeds of 40A at -48 VDC. AC-powered systems require two (redundant) circuits of 20A at 120 VAC.

Note DC systems require two redundant feeds. Cisco highly recommends uninteruptable power for both AC and DC.

The physical requirements for installation of the Cisco BTS 10200 Softswitch are documented in the *Cisco BTS 10200 Softswitch Building Environment and Power Site Survey.*

You can order the Cisco BTS 10200 Softswitch as software only, or as part of an entire Cisco Systems solution.

Software Only Purchase

When ordering the software-only solution, you will work with the Cisco BTS 10200 Softswitch product manager to determine the correct software load. The base software load includes licenses for 5,000 subscribers/DS0 licenses and 10 CPS.

If you need additional RTU and CPS, you'll need to order multiple RTU (in increments of 1K subs) and CPS licenses as appropriate.

Note Cisco TAC does not support hardware when purchased directly from Sun or another vendor. Hardware support contracts should be purchased from Sun, or their Sun Value Added Reseller.

The Sun hardware listed in can be ordered directly from the vendor. TAC will only approve the following hardware configurations.

Ordering the Hardware and Software Solution from Cisco

Hardware available from Cisco for North American Customers is listed above as the CCPU configuration. Determine if you need AC or DC, and if you want the hardware in a cabinet or ready to mount in a customer rack. Work with a BTS 10200 product manager to determine the appropriate load for your customer. This base software includes 5000 subscriber/DS0 licenses and 10 CPS.

You'll need to order RTU and CPS licenses as appropriate if additional subscribers are needed.

For more detailed information, refer to the *Cisco BTS 10200 Softswitch System Description*.

CISCO CONFIDENTIAL

Component Interoperability

Table 1 lists the supported platforms for the Cisco BTS 10200 Softswitch, and the loads that were tested for each platform.

Table 1 Component Interoperability Matrix

Supported Platform	Loads Tested Against Each Gateway
Cisco IAD 2421	c2420-a2i8sv5-mz.122-11.T4
Cisco 3640	c3640-js-mz.122-11.T2
Cisco 3660	c3660-js-mz.122-11.T2
Cisco 3660 Telco	c3660-telcoent-mz.122-11.T2
Cisco MGX 8850	vism 3.1 vism_8t1e1_003.051.001.000.fw
Cognitronics CX500 Announcement Server	M load
Cisco AS5300	c5300-js-mz.122-11.T2
Motorola CG4501	5.4.2
Thomson DHG455	1.2C.02
Cisco Universal Broadband uBR7246 Router	ubr7200-ik8s-mz.122-11.BC2.bin
Bay Packets billing server	
ESR10K	bootflash:c10k-u2p10-mz.coriolis_ios
IP Unity (2 components, below)	
Media Server	
Application Server	

Operator Access

Operator access to the Cisco BTS 10200 Softswitch is only available by secure shell (SSH) session to the EMS over Ethernet. Communications can be interactive or can be in batch mode using FTP.

Installation Notes

For detailed installation procedures for the Release 3.5 software, refer to the *Cisco BTS 10200 Softswitch Application Installation Guide*.

CISCO CONFIDENTIAL

Limitations and Restrictions

With this release, you must have secured FTP capabilities.

Note The secure FTP requirement was first implemented in Release 3.3, and has been carried over to Release 3.5.

Deactivating SS7 Links

Prior to executing the platform stop all command, Cisco recommends that you deactivate any SS7 links that are homed off of the unit. For example, if platform stop all is to be issued on the secondary side, take down the links on the secondary side first. If you are unsure which links are homed on the primary side, and which are homed on the secondary side, contact Cisco TAC for assistance. Once the maintenance is complete, reactivate the links after the Call Agent and Feature Server applications are back in service.

Transaction Queue

Ensure that the scripts used in provisioning the CA and the EMS databases are separated into pure configuration scripts, and pure control/equip scripts. Otherwise, the databases may lose synchronization. If loss of synchronization occurs, the transaction-queue may become stuck, and not clear out.

New and Changed Information

This section lists the new features and enhancements available in Release 3.5.

New Features in Release 3.5

The Cisco BTS 10200 BTS Softswitch has three new features in Release 3.5. They include:

- Small platform feature
- ISDN PRI Variant feature
- CALEA feature
- Auto Recovery of Hung CICs
- New OAMP Features
- Alarms

The following sections briefly describe these features, and how they enhance Release 3.5. For more detailed information on each of the features described here, including how to provision them, refer to the relevant Cisco BTS 10200 Softswitch Feature Modules or manuals.

CISCO CONFIDENTIAL

Small Platform Feature

The Cisco BTS 10200 Softswitch small platform is a Cisco BTS 10200 Softswitch that provides full functionality at a reduced cost, space, and call processing capacity. The benefit of the small platform is that its low cost and physically small hardware platform make it suitable for evaluations, trials, or small market deployments where initial entry costs are a factor.

Note Supporting third party hardware is NEBS Level 1 and Level 3 compliant.

The host computing system chosen as the initial target for this feature is the Sun Systems Sunfire V120 or a Netra T120, configured with 2 GB of memory for Element Management System (EMS) hosting, and 2 GB for Call Agent hosting. These memory sizes are the same as the current Cisco BTS 10200 Softswitch medium platform, and require no change to any memory-related sizing parameters. The reduced form factor host also has only one CPU.

The small platform has two differing system capacities, namely cable market (using dynamic quality of service [DQoS]) and noncable market. The numbers of subscribers and ports supported are derived numbers based on usage averages and are not hard maximum limits to be enforced. Rather, they are minimum inferred limits based on usage assumptions. The enforced ceilings are exactly the same as for the medium platform in any given release.

ISDN PRI Variant

The ISDN PRI Variant feature enhances the Cisco BTS 10200 Softswitch ISDN PRI implementation by allowing interconnection to small, and medium, businesses using legacy PBX PRI interfaces. The new design provides for the transport of additional PRI Information Elements (IEs) and two new messages. The IEs include high layer compatibility (HLC), low layer compatibility (LLC), redirecting number (RGN), original called number (OCN), and Connected Number (CN). Message support is also provided for Notify and Facility messages, and new supplementary service support is provided for the Calling Name feature.

The Cisco BTS 10200 supports all standard NI2s. Additionally, interoperability has been enhanced to also support the following new PRI variants:

- Nortel DMS-100
- AT&T 4ESS
- Lucent 5ESS

The PRI enhancements offered with this feature provide the following:

- PRI variant support for basic call handling
- Calling and Connected Name delivery
- Calling Number Identification Service (CLIP/CLIR)
- Redirecting Number support
- Improved Maintenance Message support

CALEA Feature

The Cisco BTS 10200 Softswitch provides support for Communications Assistance for Law Enforcement Act (CALEA) using two different architectures: PacketCable, and the Cisco Service Independent Intercept (SII). Release 3.5 adds support for Cisco SII. In order to support CALEA, a

CISCO CONFIDENTIAL

service provider must configure their network consistent with either the PacketCable, or the Cisco SII, network architecture using compliant network elements. It is the responsibility of the service provider to ensure that their network is CALEA-compliant.

The Cisco SII architecture provides a common architectural solution for intercept of IP communications (voice and data). It uses SNMPv3 as the control protocol and places control of lawful intercept (LI) on a mediation device (third party product) instead of on call control equipment. It also provides a common interface for mediation devices and call control equipment. Depending on your network type, you can use either the Service Independent Interception Provisioning procedure, or the PacketCable Electronic Surveillance Provisioning procedure.

Release 3.5 also supports CALEA call content reporting. Both the call data and call content are supported for call types and scenarios for basic calls and feature calls such as call forwarding, call waiting, etc. Call content allows capturing voice in a replicated RTP stream sent to the LI server by using the control commands (COPS) to the Intercept Access Points.

The Cisco BTS 10200 Call Agent provides the full CALEA functionality, Packet Cable Electronic Surveillance Specification for both call identifying information and call content (voice conversation). There are two methods of call-content used, based on the Network Architecture: Packet Cable Intercept and Service Independent Intercept.

Packet Cable Intercept

To enable the call content delivery in the network as a whole, the Edge/Aggregation Router/CMTS must support COPS, and the trunking gateway must be capable of supporting MGCP extensions for CALEA operation, especially the hairpin wiretap scenario. Additionally, SIP support at the Cisco BTS 10200 must be enhanced to support CALEA call content delivery. This is applicable for call redirection from the intercept subject that spans across multiple Call Agents.

Service Independent Intercept

To enable the call content delivery in the network as a whole, the Edge/Aggregation Router/CMTS and trunking gateway must be capable of supporting SNMP extensions for CALEA operation.

Auto Recovery of Hung CICs

Release 3.5 includes a new auditing enhancement feature—auto recovery of hung CICs. This tool audits unreachable endpoints caused from temporary network disconnectivity or congestion, and recovers the endpoints when they become reachable.

New OAMP Features

The Cisco BTS 10200 Softswitch Release 3.5 includes many new OAMP features. These features include:

- Ensuring that the collection mechanisms employed within the Cisco BTS 10200 guarantee no loss of data between collection intervals.
- Support for disabling CLI and Corba provisioning during software upgrades.
- The Cisco BTS 10200 ensuring that no calls are blocked or denied due to unavailability of billing management resources in either the call agent or EMS.
- Provisioning the allowed and disallowed standard UNIX services on the EMS and Call Agents.
- The Cisco BTS 10200 issuing applicable event reports from the Oracle DMBS engine.

CISCO CONFIDENTIAL

Alarms

There is a new alarm to monitor disk partition usage, specified by the percentage of consumption. The cause of the alarm is that a process on the system is writing too much data to a partition; when the alarm is activated, the system operator should force a switchover, and clean up the disk partition.

-

Hardware Changes in Release 3.5

The reduced physical interface is new to Cisco BTS 10200 Release 3.5. It was introduced as part of the small platform, and adds support for a network configuration consisting of two Ethernet interfaces each on the Call Agent and EMS host machines.

Cisco BTS 10200 Release 3.5 supports the current 9/5 configuration and a new reduced 2/2 configuration. Previously, the Call Agent host machine required nine Ethernet interfaces and the EMS host machine required five Ethernet interfaces.

The reduced physical interface was introduced for the for small platform configurations only. The Cisco sold hardware configuration continues to use a standard interface.

Software Changes in Release 3.5

The software changes in Release 3.5 are explained in detail in the user documentation and these release notes.

Flash Archive and Disk Mirroring

Flash archive does not work well with Disk Suite mirroring; therefore, Cisco recommends that users create the archive without disk mirroring.

Target Market and opticall.cfg

In Release 3.x, when the Target market is china in opticall.cfg, putting NOA=UNKNOWN in the dial-plan table is mandatory.

Updated Disk Replacement Procedure

The Disk Replacement procedure in the Operations Manual was updated. Please ignore the outdated Disk Replacement procedure in Chapter 1 of the Release 3.5 Operations manual, and instead use the updated procedure.

The updated procedure is located at the Updated Disk Replacement hyperlink on the *Operations Manual (Release 3.5)* index.

CISCO CONFIDENTIAL

Caveats

Caveats describe unexpected behavior in the Cisco BTS 10200 Softswitch software release 3.5.

This section describes two types of caveats:

- Open Caveats for Release 3.5, page 8
- Resolved Caveats in Release 3.5 Version 02, page 12

Open Caveats for Release 3.5

The open issues existing in Cisco BTS 10200 Softswitch software release 3.5 are described in Table 2. The DDTS ID numbers listed in Table 2 are Cisco internal tracking numbers.

Table 2 Open Caveats

DDTS ID	Description	Workaround
CSCdz67908	Policy-prefix routing is not working.	**Symptom**: Using an 800 number carrier to route an operator call (00) does not work. **Workaround**: Provision the 800 number carrier in policy-nxx table along with the translated number.

CSCdz73097	ISDN not coming in service after oos/ins.	**Symptom**: The Cisco BTS 10200 Softswitch ISDN trunk group does not come in service all the time after the following commands are sent (the ISDN trunk group remains in the out of service state):
		
		control trunk-grp id=129; mode=forced; target-state=oos;
		
		control trunk-grp id=129; mode=forced; target-state=ins;
		
		Workaround: To avoid this problem, do not execute these two commands in an immediate sequence:
		
		control trunk-grp tgn-id=129; mode=forced; target-state=oos;
		
		control trunk-grp tgn-id=129; mode=forced; target-state=ins;
		
		Wait at least one second before issuing the second command.

CSCdz73634	Platform stays in INIT state when RDM process is disabled in platform.cfg.	**Symptom**: Platform stays in “INIT” state and never exited when RDM and other processes are disabled in platform.cfg file. **Workaround**: Re-enable the RDM process in platform.cfg and restart the platform. **Note** Without the RDM process, no replication is possible. There is no reason to ever disable RDM in platform.cfg. RDM is an integral part of the platform software.

CISCO CONFIDENTIAL

Table 2 Open Caveats (continued)

DDTS ID	Description	Workaround
CSCdz74072	CA doesn't re-send service message when no ack is received.	**Symptom**: When a B ch is taken OOS, the CA sends a SERVICE message, and changes the status of the CIC to LBLK. But when no service ack is received within T323, no service message is re-sent. **Workaround**: CA needs to be switched over.
CSCdz74308	BTS10200 accepts invalid service acknowledge.	**Symptom**: We put an ISDN trunk circuit out of service via a control command (CLI). The BTS 10200 sends a service message indicating "out of service," and we respond with a service-ack message with an invalid status indication FF hex. The problem is that the bts10200 does not re-transmit the service message. This happens only on the secondary Call Agent side. Service messages are not re-transmitted. **Workaround**: Disable service messages at the ISDN trunk-grp (change isdn-tg-profile id=isdn_profile1; isdn_service_unsupp=y). **Caution** Use caution when using this workaround, as it affects many ISDN systems that rely on using service messages.
CSCdz81433	Termination table shows a status of OOS, while the trunk-termination status shows In Service.	**Symptom**: We execute the following command sequence: control trunk-termination tgn-id=129; mode=forced; cic=all; target-state=oos unequip trunk-termination tgn-id=129; cic=all equip trunk-termination tgn-id=129; cic=all control trunk-termination tgn-id=129; mode=forced; cic=all; target-state=ins control trunk-grp id=129; mode=forced; target-state=oos control trunk-grp id=129; mode=forced; target-state=ins show termination mgw-id=c2421.129; trunk-id=1 status trunk-termination tgn-id=129; source=agent; cic=all; audit termination The problem is that the termination table shows a status of OOS, while the trunk-termination status shows In Service. Doing an audit on the termination table will show that this table is corrupted after this sequence.

CISCO CONFIDENTIAL

Table 2 Open Caveats (continued)

DDTS ID	Description	Workaround
CSCdz71336	BTS10200:For G.729 Codec SS7 to SIP Interworking fails	**Symptom**: Scenario 1: SS7 to SIP Call IN CRCX BTS sends in Local Connection Options a:G.729, and not "G729", so we changed the codec string in VISM to match that and make it choose G.729a (Payload type 18) codec. Scenario 2: SIP to SS7 Call With the above config in CRCX BTS does not send anything in a: of Local Connection parameters and instead sends SDP with m=18 0 8 102, here 18 is defined as "G729" not "G.729" in an RTPmap attribute(a=rtpmap:18 G729/8000). Now with this CRCX VISM fails to understand "G729" as the codec string in VISM is "G.729". **Workaround**: The workaround is to use PCMA or PCMA as the codec used in the call.
CSCdz82534	IPCMessage pool fills up at 40cps with ss7->ss7 traffic.	**Symptom**: IPC message queue is filling up causing a switchover while running ss7->ss7 traffic at 40cps with a 180 second hold time. **Workaround**: Run the call agent at lower level of traffic.
CSCdz83047	TWC with CA switchover receive busy.	**Symptom**: After CA switchover twice, one party of a TWC goes on-hook. Then the party that originate the TWC gets busy. **Workaround**: There is no workaround at this time.
CSCdz75373	Signal stop time is not generated for call-type 24 in raw cdr file.	**Symptom**: Continuation billing records are generated for a call that is no longer active. (Continuation billing records are distinguished by the value of 1, 2, or 3 in the "Record Type" field of the billing record.) **Workaround**: Contact Cisco support to stop the continuation billing records from being generated for the non-active call.
CSCdz79111	If RKS server becomes unreachable EMA doesn’t try to re-establish a connection.	**Symptom**: Event Message (EM) billing is enabled, a single Record Keeping Server (RKS) is equipped and in service, but EMs do not get sent to the RKS. Instead, they are always written to disk. **Workaround**: Unequip the RKS by removing the radius-profile info via "change call-agent-profile". Re-equip the RKS by restoring the radius-profile info via “change call-agent-profile.” Within a few minutes, normal communication should resume. ("A few minutes" equals the value of RETRY-PRI-RKS-TIMER (in ca-config table), if defined. If not defined, it equals three minutes.)

CISCO CONFIDENTIAL

Table 2 Open Caveats (continued)

DDTS ID	Description	Workaround
CSCdz84920	QAM stopped processing Transaction.	**Symptom**: QAM Stops processing the transaction given from CLI. **Workaround**: The workaround for this is to follow these steps: 1. Login to primary (active) EMS using the root account 2. Execute the "pkill qam" directive at the command prompt.
CSCdz90189	Snmpwalk on entire branch fails due to the bulk status, 5296.1.8 branch.	**Symptom**: Snmpwalk on the entire opticall branch fails due to the walk not being able to exit gracefully from the 5296.1.8. **Workaround**: The workaround for this is to follow these steps: 1. Login into active EMS as root. 2. "pkill sad" 3. Wait 10 seconds for process to reinitialize. 4. Perform snmpwalk on branch .1.3.6.1.4.1.5296.1.8 at least once every 12 hours.

CISCO CONFIDENTIAL

Resolved Caveats in Release 3.5 Version 02

Resolved caveats listed in this section include only those critical and major caveats that were found during system test or critical issues found during customer verification tests of earlier releases and resolved in Release 3.5 Version 02. The DDTS ID numbers listed in Table 5 are Cisco internal tracking numbers.

Resolved caveats listed in this section include only those critical and major caveats that were found during system test or critical issues found during customer verification tests of earlier releases and resolved in Release 3.5. The DDTS ID numbers listed in Table 5 are Cisco internal tracking numbers.

Table 3 Resolved Caveats for Release 3.5 Version 02

DDTS ID	Description
CSCea13479	Table Policy_prefix not populated in shared mem from 2.1>3.5.
CSCea13765	ISA process dies while runing 7cps for a few hours.
CSCea13767	Trunk-grp id range of 13 to >9000000 causes adm to continually restart.

Resolved Caveats in Release 3.5 Version 01

Resolved caveats listed in this section include only those critical and major caveats that were found during system test or critical issues found during customer verification tests of earlier releases and resolved in Release 3.5 Version 01. The DDTS ID numbers listed in Table 4 are Cisco internal tracking numbers.

Table 4 Resolved Caveats for Release 3.5 Version 01

DDTS ID	Description
CSCea05415	Update EMS table sizing provisioning script with updated requirement.

Resolved Caveats in Release 3.5 Version 00

Resolved caveats listed in this section include only those critical and major caveats that were found during system test or critical issues found during customer verification tests of earlier releases and resolved in Release 3.5 Version 00. The DDTS ID numbers listed in Table 5 are Cisco internal tracking numbers.

Table 5 Resolved Caveats for Release 3.5 Version 00

DDTS ID	Description
CSCdx03210	Database backup procedures need to INFOrm success (send events).
CSCdy12366	Pri orig to CIDCW active line - No CID/CNAM info displayed.
CSCdy20432	blg2 heap memory growing in size with soak run.
CSCdy26241	BTS 10200 not sending Error when it receives RSIP with same txnId in 2 minutes.
CSCdy27601	CDR ANI is incorrect when no ANI on incoming call.
CSCdy29584	Billing shows wrong CALLTERMCAUSE when TWC interworks with SCR.

CISCO CONFIDENTIAL

Table 5 Resolved Caveats for Release 3.5 Version 00 (continued) (continued)

DDTS ID	Description
CSCdy41492	mgw-monitoring always performs a DNS query.
CSCdy46881	Multiple KAM: Mate side has become Faulty alarms do not clear.
CSCdy65129	BTS does not send right cause value in Call-Proceding.
CSCdy72515	Bad_error_number log is generated for SUBSCRIBER_FEATURE_DATA ACTIVE=NULL.
CSCdy88021	No value on Received msg from TCA on a free idx. for announcement message.
CSCdz03475	Critical database alarm generated for alert.log shows deadlock detected.
CSCdz06694	/opt become full, BDMS stopped generating CDR logs.
CSCdz08090	Connection is not cleared upon 502 Active connection exists.
CSCdz09304	ISDN local call mapped to CdPN TON=3 (network specific).
CSCdz15522	Hardware Monitor should monitor /var and flex alarm levels.
CSCdz15547	Oracle generating a critical alarm the should be a minor.
CSCdz16674	CRCX_ACK was not reported to CNM for dollar CRCX.
CSCdz17336	Ability to configure Start Transit/Stop Pulse for CAS MO Package.
CSCdz20056	Lost of dial-tone after recovery from lost of IP connectivity.
CSCdz20776	CFB call does not strip off NDC of orig calling party.
CSCdz20947	Annc trks are idle, calls get busy, annc trks hang.
CSCdz22447	NO OLI with Charge information on IAM.
CSCdz23958	BTS should implement both rt@connectionID and rbk(xxx).
CSCdz24058	Capital Xs in OFFICE-CODE cause call failure.
CSCdz24722	Call Agent passes call on a termination with SS7 CIC table error.
CSCdz24763	EMS gives Network Device Already in Use Errors Statusing Subscribers.
CSCdz27483	BTS send NOA=1110010 for 0+7 ss7 call.
CSCdz37767	Performance improvement: replace process_malloc with malloc.
CSCdz37780	Performance improvement: get rid of lock/unlock while allocating TIDs.
CSCdz39159	IPCMsg priority of MGCP Stack Timer message needs to be increased.
CSCdz47092	tga process sticks in loop causing CPU utilization to increase.
CSCdz50546	PRI inbound call fails when preferred channel ID not selected.
CSCdz52457	EMS dies due to max HB period when hub is overloading CPU.
CSCdz57918	Call failures after 2 consecutive cot failures.
CSCdz58314	Attribute count on Service Instance has wrong value.

CISCO CONFIDENTIAL

Documentation Updates

The following Cisco BTS 10200 documents were modified to reflect the new information for Release 3.5:

- *Cisco BTS 10200 Softswitch Physical and Network Site Surveys and Data Sheets*
- *Cisco BTS 10200 Softswitch Cabling Procedures*
- *Cisco BTS 10200 Softswitch Application Installation Procedures*
- *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*

These new feature modules were also added to the Cisco BTS 10200 documentation set:

- The Cisco BTS 10200 Softswitch Release 3.5 CALEA Feature Module (OL-3422-02)
- Cisco BTS 10200 Softswitch Release 3.5 ISDN PRI Variant Feature Module (OL-3421-01)
- Cisco BTS 10200 Release 3.5 Small Platform Feature Module

Note The Cisco BTS 10200 Softswitch user documentation is password protected. Consult your Cisco representative for access.

Related Documentation

For more information about the Cisco BTS 10200 Softswitch, refer to the following Cisco BTS 10200 Release 3.*x* documents:

- *Cisco BTS 10200 Softswitch Physical and Network Site Surveys and Data Sheets*
- *Cisco BTS 10200 Softswitch Cabling Procedures*
- *Cisco BTS 10200 Softswitch Application Installation Procedures*
- *Cisco BTS 10200 Softswitch Jumpstart Server Procedures*
- *Cisco BTS 10200 Softswitch System Description*
- *Cisco BTS 10200 Softswitch Operations Manual*
- *Cisco BTS 10200 Softswitch Event Messages and Alarms Reference Guide*
- *Cisco BTS 10200 Softswitch Billing Interface Guide*
- *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*
- *Cisco BTS 10200 Softswitch CORBA Installation and Programmer's Guides*

All Cisco BTS 10200 Softswitch user documentation can be accessed through the following location:

http://www.cisco.com/univercd/cc/td/doc/product/voice/bts10200/index.htm

CISCO CONFIDENTIAL

Cisco BTS 10200 Release 3.5 Feature Modules

The following are the feature modules written for Cisco BTS 10220 Release 3.5:

- The Cisco BTS 10200 Softswitch Release 3.5 CALEA Feature Module (OL-3422-02)
- Cisco BTS 10200 Softswitch Release 3.5 ISDN PRI Variant Feature Module (OL-3421-01)
- Cisco BTS 10200 Release 3.5 Small Platform Feature Module

Cisco BTS 10200 Release 3.*x* Feature Modules

The following feature modules were written for Cisco BTS 10220 Release 3.*x*:

- *Cisco BTS 10200 Softswitch Release 3.3 PacketCable Feature Module*
- *Cisco BTS 10200 Softswitch CALEA Release 3.3 Feature*
- *Cisco BTS 10200 Softswitch Release 3.3 Automatic Callback, Automatic Recall Feature*

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

Note Documentation for the Cisco BTS 10200 Softswitch on the World Wide Web sites listed above is currently available only through password access. Contact your Cisco representative for assistance.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Note Documentation for the Cisco BTS 10200 Softswitch is not currently available on the Documentation CD-ROM.

Ordering Documentation

Cisco documentation is available in the following ways:

CISCO CONFIDENTIAL

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order Documentation CD-ROMs through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can also e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Attn Document Resource Connection
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

CISCO CONFIDENTIAL

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

Contacting TAC by Telephone

If you have a priority level 1(P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

CISCO CONFIDENTIAL